Data Protection Office

AN OVERVIEW OF THE DATA PROTECTION ACT 2017

Presented By:
Mrs. R. Goburdhun and Mrs W. Khadun

Data Protection Officer/Senior Data Protection Officer
24 July 2019

Agenda

- Aims of the Data Protection Act 2017 (DPA)
- Benefits of the Act
- The Data Protection Office
- Functions of the Data Protection Office (DPO)
- Basic Concepts
- Application of the Act
- Obligations on Controllers and Processors
- Rights of data subjects
- Offences and penalties
- Certification

Aims of the DPA

- Came into force on 15 January 2018

To strengthen the control and personal autonomy of data subjects (individuals) over their personal data

In line with the European Union's General Data Protection Regulation (GDPR)

To simplify the regulatory environment for business in our digital economy.

To promote the safe transfer of personal data to and from foreign jurisdictions

Benefits of the Act

- Increased accountability of controllers
  - Implement better processes
  - Better organisations
  - Better productivity
  - Strengthen customer trust
  - Gain confidence and trust

- Enhanced data subjects' rights of individuals for greater control over their personal data.

- Improve the digital legal landscape to respond to the new EU requirements for adequacy, thereby attracting foreign investors.

- Minimised risk of data breaches

The Data Protection Office

The Data Protection Office (DPO)

- Public office which acts with complete **independence** and **impartiality**.
- Not subject to the control or direction of any other person or authority in the discharge of its functions.
- Head of the Office is the **Data Protection Commissioner**.

Functions of DPO

I	• ENSURE COMPLIANCE WITH DPA 2017 AND REGULATIONS
II	• REGISTRATION OF CONTROLLERS AND PROCESSORS
III	• INVESTIGATION OF COMPLAINTS
IV	• SENSITISATION/ TRAINING
V	• EXERCISE CONTROL ON ALL DATA PROTECTION ISSUES
VI	• CONDUCT DATA PROTECTION COMPLIANCE AUDITS
VII	COOPERATE WITH SUPERVISORY AUTHORITIES OF OTHER COUNTRIES
VIII	• RESEARCH ON DATA PROTECTION

Basic Concepts

Section 2 - Interpretation

Basic Concepts

Data Subject

- an identified or identifiable individual (any data which can identify an individual),
- in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Personal Data

- any information relating to a data subject

Basic Concepts

Processing

- an operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as, collection, recording, organisation, structuring, storage, restriction, erasure or destruction, use, etc.

Basic Concepts

Controller

- a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing

Processor

- a person who, or a public body which, processes personal data on behalf of a controller.

Application of the Data Protection Act

Section 3

Application of the Act (1)

For the purposes of this Act, each Ministry or Government department will be treated as separate from any other Ministry or Government department.

This Act applies to the processing of personal data, wholly or partly, by automated means and to any processing otherwise than by automated means where the personal data forms part of a filing system or is intended to form part of a filing system.

Application of the Act (2)

The Act applies to a controller / processor who:

is established in Mauritius and processes personal data in the context of that establishment; and

is not established in Mauritius but uses equipment in Mauritius for processing personal data, other than for the purpose of transit through Mauritius.

Non - Application of the Act

The Act does not apply to:

the exchange of information between Ministries, Government departments and public sector agencies where such exchange is required on a need-to-know basis;

the processing of personal data by an individual in the course of a purely personal or household activity.

Obligations on controllers and processors

Sections 21 to 33

Obligations on controllers and processors

Registration and renewal as controller and/or processor (s 14)	1. Application forms available on DPO website. 2. Guidance on registration and renewal on DPO website.
Comply with the 6 principles for processing personal data (s 21)	1. Lawful, fair and transparent 2. Purpose limitation 3. Data minimisation 4. Data accuracy 5. Storage limitation 6. In accordance with the rights of data subjects.
Duties of controller (s 22)	1. Adopt policies and implement appropriate data security and organisational measures. 2. Designate a Data Protection Officer. 3. Verify the effectiveness of measures implemented.
Collection of personal data (s 23)	Done for a lawful purpose and is necessary.
Conditions for consent (s 24)	1. A controller bears the burden of proof for establishing consent. 2. An individual can withdraw his consent anytime. 3. Consent is presumed not freely-given if the performance of a contract/service is dependent on the consent which is not necessary for such execution of the contract/service.

Obligations on controllers and processors

Notification of personal data breach (s 25)	**1. To notify the Data Protection Office where feasible not later than 72 hours after becoming aware.** **2. Form available on DPO website.**
Communication of breach to data subject (s 26)	**Where it is likely to result in a high risk to the rights and freedoms of the data subject.**
Duty to destroy personal data (s 27)	**1. To destroy personal data as is reasonably practicable when the purpose has lapsed.** **2. To notify any processor holding the data for destruction.** **3. Retention period has to be determined by controllers taking into account the purpose and other applicable laws.**
Lawful processing (s 28)	**Must meet at least one criteria for lawful processing.** 9 criteria – (1) consent (2) contract (3) legal obligation (4) vital interest of data subject (5) official authority vested in the controller (6) a task carried out by a public authority (7) exercise, by any person in the public interest, of any functions of a public nature (8) legitimate interests of the controller which do no override the rights and freedoms of data subjects (9) historical/statistical or scientific research.
Special Categories of personal data (s 29)	**Must implement specific protection and a stricter regime.**
Personal data of child (s 30)	**Parental or guardian consent must be obtained for processing the personal data of children under the age of 16.**

Obligations on controllers and processors

Security of processing (s 31)	**Implement appropriate security and organisational measures.**
Record of processing operations (s 33)	**Template available on DPO website.**
Processing operations likely to present risk to individuals (s 34&35)	**1. Guidance on how to evaluate high risk processing operations.** **2. Perform a DPIA.** **3. DPIA form available on DPO website.** **4. Comply with the requirements for prior authorisation from, or consultation with the Commissioner.**
Transfer of personal data outside Mauritius (s 36)	**Transfer may be made provided that the transfer is :** • **subject to suitable safeguards put in place** • **made with the individual's informed consent;** • **necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;** • **necessary for the performance of a contract made in the interests of the individual between the controller and another person;** • **necessary for important reasons of public interest;** • **necessary for the establishment, exercise or defence of legal claims;** • **necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or** • **necessary for the purposes of the compelling legitimate interests of the controllers(provided such interests are not overridden by the interests of the individual);**

Prior security check – Section 32

- Provides for the power of the Data Protection Commissioner to perform security checks and inspection of the security measures imposed on the controller or processor.

Rights of Data Subjects

Sections 37 to 41

Rights of Data Subjects

Right of access – S37

- A data subject has the right to obtain confirmation that his/her personal data is processed and a copy of the data free of charge within one month following a written request.

Automated individual decision making – S38

- A data subject has the right not to be subject to a measure which is based on profiling by means of automated processing.

Rectification –S39

- A data subject has the right to obtain from controller rectification of inaccurate or incomplete personal data concerning him/her without undue delay.

Rights of Data Subjects

Erasure – S39

- Data subject may request that his/her personal data are erased without undue delay if the continued processing of those data is not justified.

Restriction of Processing – S39

- A data subject may request that the processing of his/her personal data is restricted where the accuracy of the data is contested or he/she requires it for a legal claim amongst others.

Object – S40

- A data subject has the right to object in writing at any time the processing of personal data relating to him/her free of charge.

Exercise of rights – Section 41

- Where a person is a minor or physically or mentally unfit, a person duly authorised (parents, guardian, legal administrator) can exercise their rights on their behalf under this part.

OTHER OFFENCES AND PENALTIES

Sections 42 and 43

Unlawful disclosure of personal data – Section 42

Controller	Any controller who, without lawful excuse, discloses personal data in any manner that is incompatible with the purpose for which such data has been collected shall commit an offence.
Processor	Any processor who, without lawful excuse, discloses personal data processed by him without the prior authority of the controller on whose behalf the data are being or have been processed shall commit an offence.

Offences and Penalties – Section 43

There are various offences and criminal penalties under this Act which, in general, if committed, are sanctioned by a court of law.

Where no specific penalty is provided, any person who does not comply or contravenes this Act shall, on conviction, be liable to a fine not exceeding 200,000 rupees and to imprisonment for a term not exceeding 5 years.

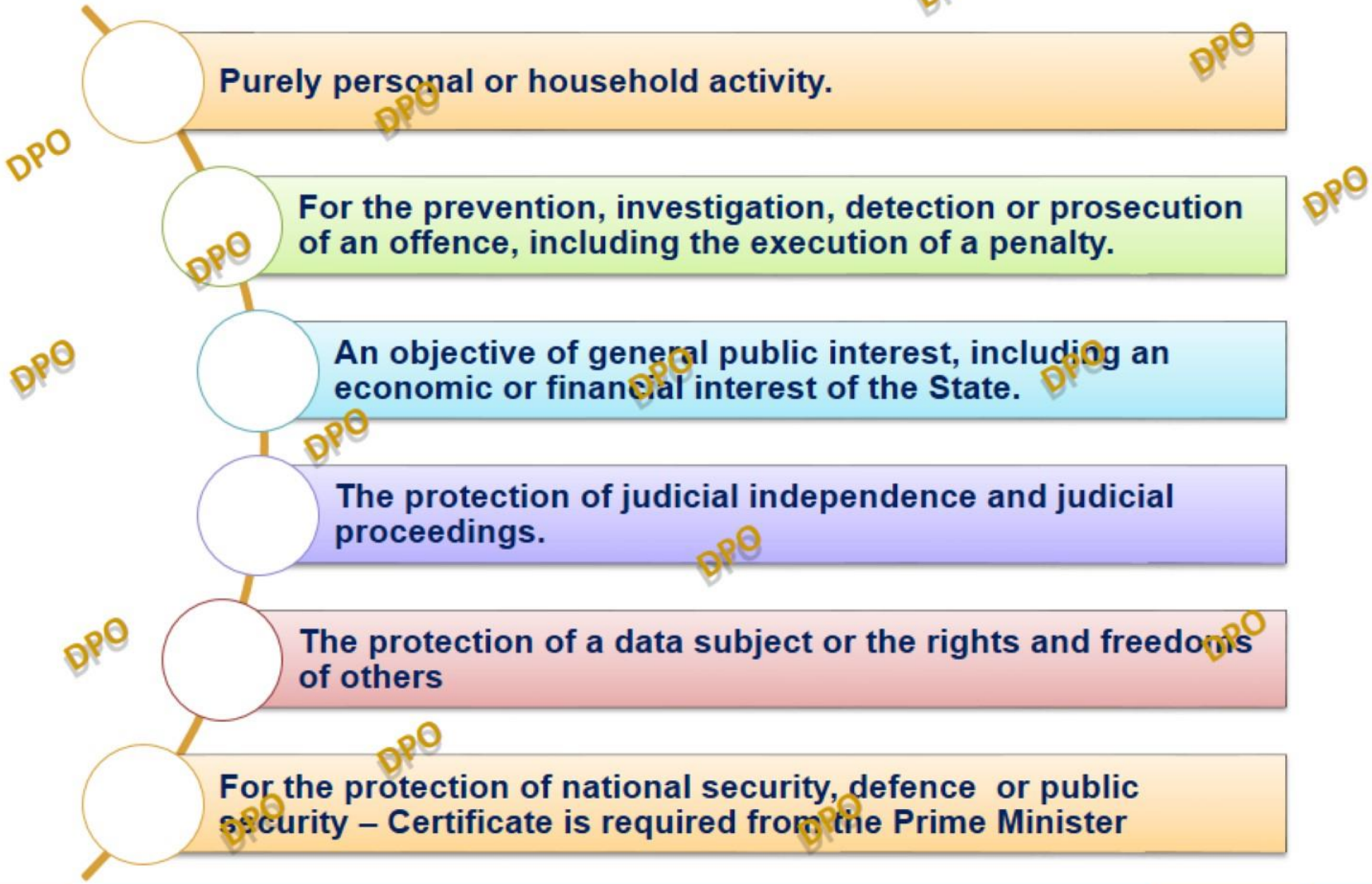
Other Offences and Penalties

Offences	Penalties
Section 6: Investigation of Complaints Any person who fails to attend a hearing or to produce a document or other material when required to do so.	Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.
Section 7: Power to require information Any person who fails or refuses to comply with a requirement specified in a notice, or who furnishes to the Commissioner any information which he knows to be false or misleading in a material particular.	Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.
Section 15: Application for registration Any controller or processor who knowingly supplies any information, during registration, which is false or misleading in a material particular.	Liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.
Section 17: Change in particulars Any controller or processor who fails to notify a change in particulars.	Liable to a fine not exceeding 50, 000 rupees.
Section 28: Lawful processing Any person who process personal data unlawfully.	Liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.

EXCEPTIONS AND RESTRICTIONS

Sections 44

Exceptions and Restrictions – S44



CERTIFICATIONS

Section 48

Certification – Section 48

- To enhance transparency and compliance with the Data Protection Act 2017, certification

  - helps controllers or processors to demonstrate accountability and compliance with the Act
  - builds confidence and trust in the organisation with all stakeholders, as well as with the wider public
  - allows data subjects to quickly assess the level of data protection of relevant products and services
  - gives legal certainty for cross-border data transfers

Certification – Section 48

Certification body	• Certification will be issued by the Data Protection Office.
Compulsory and Fee?	• Certification is voluntary and free.
Validity	• Certification is valid for three years and is subject to renewal. Controllers or processors may apply for renewal of the certification before the date of its expiry.
Withdrawal	• Certification is subject to withdrawal where the conditions for issuing the certification are no longer met.

Thank you

Any questions?

Contact us:

Website : http://dataprotection.govmu.org

Email: dpo@govmu.org

Tel: 4600251